REMARKS

Submitted herewith is an Excess Claims Fee Payment Letter.

Claims 1-46 are all the claims presently pending in the application. New claims 38-46 have been added to more completely define the invention.

Claims 1-35 stand rejected upon informalities (e.g., 35 U.S.C. § 112, first and second paragraph) and claims 1-5, 8, 11, 12, 15, 19, 20, 22, 23 and 34-37 stand rejected on prior art grounds. Claim 1-35 have been amended in a manner believed fully responsive to all points raised by the Examiner.

It is noted that the claims have been amended solely to more particularly point out Applicant's invention for the Examiner, and not for distinguishing over the prior art, narrowing the claim in view of the prior art, or for statutory requirements directed to patentability.

It is further noted that, notwithstanding any claim amendments made herein, Applicant's intent is to encompass equivalents of all claim elements, even if amended herein or later during prosecution.

Attached hereto is a marked-up version of the changes made to the claims by the current Amendment. The attached pages are captioned "**Version with markings to show changes made**".

Claims 1-3, 8, 11, 12, 15, 19, 20, 23 and 34-37 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Linehan (U.S. Pat. 6,327,578) (hereinafter "Linehan").

Claims 1-3 and 34-37 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Low et al (U.S. Pat. 5,420,926) (hereinafter "Low").

Claims 1-3, 15, 19, 23, 35, 36 and 37 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Gabber et al (U.S. Pat. 5,961,593) (hereinafter "Gabber").

Claims 4, 5 and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Linehan in view of Holloway (U.S. Pat. 5,604,802)(hereinafter "Holloway").

These rejections are respectfully traversed in view of the following discussion.

I. THE CLAIMED INVENTION

Applicant's invention, as defined for example in independent claim 1 (and substantially similarly in independent claims 2, 24, 34, 35, 36, and 37) is directed to a system (and method) for

conducting business electronically between a first party and a second party including providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties, conducting the electronic business transaction between the first and second parties through the third party such that the identity of the first party is kept from the second party.

A feature of the present invention, in a non-limiting embodiment as defined by independent claim 1, is that the second party is only able to identify the first party as a counterpart in the electronic business transaction.

With such features, potential customers perceive and are provided increased privacy and security associated with electronic commerce while the business entity is provided with some level of business intelligence (e.g. see 16-20 and page 17, lines 1-2).

An exemplary configuration of the system and method for a system (and method) for conducting business electronically between a first party and a second party is shown in Figs. 1-5 of the application.

The conventional systems, such as those discussed below and in the Related Art section of the present application, do not have such a structure, and fail to provide for such an operation.

II. THE PRIOR ART REFERENCE

A. The Linehan Reference

Firstly, Applicant respectfully submits that the Examiner's assertions regarding Linehan are erroneous.

Specifically, Linehan discloses a protocol in which a customer and structure in which "*The consumer authenticates to the consumer's own issuing bank.....[t]he merchant's certificate should identify the acquiring bank that holds the merchant's business account used to settle payments*" (e.g., see column 11, lines 48-65 of Lineham). Thus, in Lineham there is a consumer, a merchant, a consumer bank, and a merchant's bank. In Lineham, the consumer bank authenticates the consumer, the merchant's bank authenticates the merchant, and the consumer bank and the merchant bank authenticate each other. Further, in Linehan, as shown in Figs. 1,

2A, 2B, 2C, 4, 5, and 6, the consumer and the merchant are in direct contact with each other and their identities are known to each other. Thus, Linehan does not teach or suggest the present invention.

In sharp and fundamental contrast in the present invention is "*conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party*", as defined by independent claim 1 (and substantially similarly by independent claims 2, 24, and 34-37). This is completely opposite from the protocol of Linehan.

Further, in the present invention "*said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction*". This is much different from Linehan where the consumer contacts the merchant directly (e.g., computer to computer) in a start sequence.

For the reasons stated above, claims 1-3, 8, 11, 12, 15, 19, 20, 23 and 34-37 of the claimed invention are fully patentable over Linehan.

B. The Low Reference

However, similar to the assertions regarding Linehan, Applicant submits that the Examiner's assertion that Low anticipates the present invention are also erroneous.

That is Low also describes a 4-way protocol of a customer C, a credit card issuing bank, a bill paying bank, and a store S which is being paid. While Low teaches that the billpaying bank may not know the customer on whose behalf the bills are paid, the same can not be said of the store (e.g., merchant). The store has a credit card purchase device which reads the customer's credit card. Therefore the consumer and the merchant are in direct contact with each other and their identities are known to each other. Further, the bill paying bank is in a merchant relationship with the credit card issuing bank which is the customer.

In contrast, in the present invention is "*conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party*", as defined by independent claim 1 (and substantially similarly by independent claims 2, 24, and 34-37).

Further, in the present invention "*said second party is provided with information*

identifying said first party only as a transactional party in said electronic business transaction". This is much different from Low where the customer C contacts the store S directly (e.g., physically purchasing goods).

For the reasons stated above, claims 1-3 and 34-37 of the claimed invention are fully patentable over Low.

C. The Gabber Reference

However, similar to the assertions regarding Linehan and Low, Applicant submits that the Examiner's assertion that Gabber anticipates the present invention is also erroneous.

Gabber discloses to a system and method allowing a user to browse personalized server resources on a network anonymously. However Gabber does not disclose not providing "*privacy-compromising information regarding a proposed electronic business transaction between the first and second parties*", as define by independent claim 1 (and substantially similarly by independent claims 2, 24, and 35-37). Instead, Gabber discloses a browser for "*(accessing, locating, retrieving, reading, contacting, etc.) the sites*" (e.g., see column 2, lines 64-65 of Gabber). This is completely different from entering into a proposed electronic business transaction between parties.

Further, Gabber nowhere discloses "*wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction*", as defined by independent claim 1 (and substantially similarly by independent claims 2, 24, and 34-37).

For the reasons stated above, claims 1-3, 15, 19, 23, 35, 36 and 37 of the claimed invention are fully patentable over Gabber.

Hence, turning to the clear language of the claims, there is no teaching or suggestion by Linehan, Low, and Gabber of "*[a] method of conducting business electronically between a first party and a second party, comprising:*

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties

through the third party such that said identity of said first party is kept from the second party.

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction (emphasis Applicant's).

Additionally new claims 38-46 define additional novel and non-obvious limitations.

Further, regarding the §103(a) rejection of claims 4, 5 and 22 as being unpatentable over over Linehan in view of Holloway, when combined with independent claim 1, these claims also define additional novel and non-obvious features.

Further, the other prior art of record has been reviewed, but it too even in combination with Linehan, Low, Gabber, and Holloway, fails to teach or suggest the claimed invention.

III. FORMAL MATTERS AND CONCLUSION

Regarding the Examiner's objection to the specification on page 8, line 10, Applicant respectfully notes that the pu1(I) belonging to the key (Pr1(I),pu1(I)) is the public signature scheme of I (e.g., insurance entity). The sequence pu2(I,C) is the public part of a public encryption scheme (Pr2(I,C),pu2(I,C) computed by the customer C. C communicates pu2(I,C) together with her/his application. Applicant submits that the specification is clear as written.

Regarding the Examiner's objection to the Drawings, Applicant herewith submits a Submission of Proposed Drawing Corrections to show proposed corrections to Figure 1 marked in red.

In view of the foregoing, Applicant submits that claims 1-46, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: 11/08/02

Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
Intellectual Property Law
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254

CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that I am filing this Amendment by facsimile with the United States Patent and Trademark Office to Examiner M. Huseman, Group Art Unit 3621 at fax number (703) 305-7687 this 8th day of November, 2002.

Sean M. McGinn, Esq.
Registration No. 34,386

IN THE SPECIFICATION:

Please replace the paragraph on page 1, line 12 to page 2, line 4, with the following paragraph:

-- However, in reality, several policies and technologies exist which allow to use the benefits of electronic commerce with complete protection of privacy and even complete anonymity. For instance, protocols for anonymously buying solid goods and electronic goods have been disclosed respectively in U.S. Patent Application No. 09/129,826, filed on August 5, 1998, entitled "Method and apparatus for remote commerce with customer anonymity", by M. Shub et al. , and in U.S. Patent Application No. [09/___,___,] 09/569,068 filed on May 11, 2000, entitled "Achieving Buyer-Seller Anonymity for Unsophisticated Users Under Collusion Amongst Intermediaries" by P. Dubey et al.. However, despite these advances in security, there is still a perceived lack of privacy and security in performing e-commerce by a wide majority of potential users. --

Please replace the paragraph on page 7, lines 7 to 15 with the following paragraph.

-- The device P(C) delivers a serial number S(C) at each transaction, and S(C) can be read off P(C) only in the presence of customer C. For more privacy, it would be better that P(C) generates numbers S(C,n), where n is an integer belonging to a large set {1,2,...,N}. Then, for each new insurance company and or other partner of customer C, a new number n is chosen as a starting number for all further transaction(s) between the two parties. In particular, if C quits insurance entity I for another company and comes back to I, it can change the n associated to I. For simplicity, the use of this number n will be omitted in the sequel, as using it is a trivial amelioration of the overall protocol. –

Please replace the paragraph on page 7, line 16 to page 8, line 4, with the following paragraph.

-- The insurance entity I will also choose a large set of verifiers Vj, j=1, 2,... which will be

medical [practices] practitioners for health (or life) insurance, and garages in the case of automobile insurance. Any verifier will be equipped with the apparatus needed to verify portable devices as described above, and will be connected to the Internet so that they can send information to third party T. The relation with T can be performed using a privacy protection mechanism, involving several other parties to avoid possible collusion, as described for instance in the home page of the NetBill Security and Transaction Protocol by B. Cox, J.D. Tygar, an M. Sirbu which can be obtained on the Internet at [http://www.ini.cmu.edu/netbill]www.ini.cmu.edu/netbill: see the paper "Maintaining privacy in electronic transactions" by Benjamin T.H. Fox. These are referred to collectively as "Ref3". –

Please replace the paragraph on page 8, lines 5 to 14 with the following paragraph.

-- When deciding to register with insurance I, customer C sends to T an application A. This application can be taken off, for example, the world-wide-web (WWW) page of the business (insurance) entity I, together with a piece of software SOFT, such as a JAVA applet, which allows [to encrypt] encryption using pu1(I) where (Pr1(I),pu1(I)) is the public signature scheme of I. SOFT also allows customer C to compute a public signature scheme (Pr2(I,C),pu2(I,C)). C will communicate pu2(I,C) together with her/his application, or other form of first contact through T. As pu2(I,C) is the public part of a public encryption scheme, there is very limited risk in T knowing that key. For improved security, pu2(I,C) can be encrypted using pu1(I) before being communicated to I through T. --

IN THE CLAIMS:

Please amend the claims as follows.

1. (Amended) A method of conducting business electronically between a first party and a second party, comprising:

providing an intermediary relationship with a third party who knows an identity of the first party but no privacy-compromising information regarding a proposed electronic business

transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party,

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

2. (Amended) A method of performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer, to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party,

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction.

6. (Amended) The method according to claim 5, wherein said portable device P(C) generates numbers S(C,n), where n is an integer belonging to a set {1, 2, . . . , N}, and wherein for at least one of [each] a new business unit and [other] another partner of the customer, a new number n is chosen for all further [transaction] transactions between the customer and said at least one of [each] said new business unit and [other] said another partner.

7. (Amended) The method according to claim 2, wherein the business entity chooses a set of verifiers Vj, j = 1, 2, . . .N, ,

wherein said verifiers are each equipped to verify portable devices, and are connectable to a network so as to output information to [the] a third party T using privacy protection.

8. (Amended) The method according to claim 2, wherein said establishing an intermediary

relationship includes sending by [when deciding to register with a business entity,] the customer [sends] to the third party an application to register with said business entity and [a] software to encrypt the application using a public key pu1(I) included in [where (Pr1(I),pu1(I)) is] a public signature scheme (Pr1(I),pu1(I)) of the business entity,

said software further allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), said application being provided over a network connected to said business entity.

15. (Amended) The method according to claim 2, wherein, with a relationship between the customer and the business entity previously established, the business entity interacts with the customer [despite not knowing an identity of customer] identified as a counterpart.

24. (Amended) A method of selecting a purveyor of goods or services in a confidential manner over a network, comprising:

sending, by a customer, an application to a third party along with software which allows encrypting the application using a public key pu1(I),

wherein said application is taken electronically from a business entity[, along with a code which allows encrypting the application using a public key pu1(I)],

[where (Pr1(I),pu1(I)) is] wherein a public signature scheme of said business entity is (Pr1(I),pu1(I)), said [code] software allowing the customer to compute a public signature scheme (Pr2(I,C),pu2(I,C)), and

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic business transaction.

34. (Amended) A system for conducting business electronically between a first party and a second party, comprising:

means for providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first party and second [parties] party; and

means for conducting the electronic business transaction between said first party and second [parties] party through the third party such that said identity of said first party is kept from

the second party.

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

35. (Amended) A signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for conducting business electronically between a first party and a second party, said method comprising:

providing to a third party an identity of the first party but no privacy-compromising information regarding a proposed electronic business transaction between the first and second parties; and

conducting the electronic business transaction between said first and second parties through the third party such that said identity of said first party is kept from the second party.

wherein said second party is provided with information identifying said first party only as a transactional party in said electronic business transaction.

36. (Amended) A system for performing electronic commerce without a candidate customer being forced to disclose private data together with an identity of the candidate customer to a business entity requiring said private data, said system comprising:

means for establishing an intermediary relationship with a third party between the candidate customer and the business entity;

a proprietary item provided to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

means for performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity party.

wherein said business entity is provided with information identifying said candidate customer only as a transactional party in said electronic commerce.

37. (Amended) A signal-bearing medium tangibly embodying a program of machine- readable instructions executable by a digital processing apparatus to perform a method of performing electronic commerce without a candidate customer being forced to disclose private data together

with an identity of the candidate customer to a business entity requiring said private data, said method comprising:

establishing an intermediary relationship with a third party between the candidate customer and the business entity;

providing a proprietary item to said customer such that the customer can be identified as a legitimate owner of the item without revealing the identity of said customer; and

performing electronic commerce between said customer and said business entity through said third party, utilizing said proprietary item, such that an identity of said customer is kept from said business entity.

wherein said business entity is provided with information identifying said customer only as a transactional party in said electronic commerce.